Math 357
Expositional homework 02

Assigned: 2024–01–22 (M)
Due: 2024–02–08 (R)

The goal of this homework is to recall ideas from general ring theory and engage them in the specific setting of polynomial rings. The exercises are adapted from Dummit & Foote, 3e, Exercises 9.2.1–5.

Let F be a field, let t be an indeterminate over F, and let $f \in F[t]$.

(a) Let $\deg f = n \geqslant 1$. For each $g \in F[t]$, let $\overline{g}$ denote the residue of g under the natural projection map $\varphi : F[t] \to F[t]/(f)$. Prove that for each $\overline{g} \in F[t]/(f)$ there exists a unique polynomial $g_0 \in F[t]$ such that $\deg g_0 \leqslant n-1$ and $\overline{g}_0 = \overline{g}$.

(b) Prove that $F[t]/(f)$ is a field if and only if f is irreducible.

(c) Let $f = \prod_{i=1}^{n} p_i$ be a factorization of f into irreducible elements. Describe all ideals in the ring $F[t]/(f)$, in terms of the p_i.

(d) Prove that $F[t]$ has infinitely many prime elements. *Hint:* See Exercise 9.2.4 (p 301).

(e) Further assume that F is a finite field, of order q. Let $\deg f = n \geqslant 1$. Prove that $F[t]/(f)$ has exactly q^n elements. *Hint:* Explain how to view the result of Exercise (a) in the framework of vector spaces. See Exercise 9.2.1 (p 301).

Solutions

Exercise (a)

Note that, despite what loose use of notation may lead us to think, $\overline{g} \in F[t]/(f)$ is a *coset* $g + (f)$, not an *element* $g_0 \in F[t]$. Specifically, $\overline{g}$ is not the remainder g_0 when dividing g by f. This exercise essentially asks us to show that we may identify g_0 with $\overline{g}$.

In our argument below, notice how almost everything we want comes from the division algorithm on $F[t]$ associated with the norm on $F[t]$ induced by the degree function.

Our first step is to associate to each coset $\overline{g}$ a polynomial $g_0 \in F[t]$ with the desired properties. Let $\overline{g} \in F[t]/(f)$, and choose any coset representative $g \in \overline{g}$. (Note that $g \in F[t]$.) By the division algorithm on $F[t]$,[1] there exist unique $q_g, r_g \in F[t]$ such that

$$g = q_g f + r_g \tag{1}$$

[1] See DF3e, p 299.

with $r_g = 0$ or $\deg r_g < \deg f = n - 1$.[2] We may rewrite equation (1) as $g - r_g = q_g f \in (f)$, so $g + (f) = r_g + (f)$; that is, $\overline{g} = \overline{r}_g$.

We claim r_g is independent of the choice of coset representative. To see this, let $g_2 \in \overline{g}$ be any coset representative. Then $g + (f) = \overline{g} = g_2 + (f)$, if and only if $g_2 - g \in (f)$, if and only if there exists some $q \in F[t]$ such that $g_2 = qf + g$. By the division algorithm on $F[t]$, there exist unique $q_2, r_2 \in F[t]$ such that

$$g_2 = q_2 f + r_2$$

with $r_2 = 0$ or $\deg r_2 < \deg f$. From our work above, we also have

$$(q + q_g)f + r_g = qf + q_g f + r_g = qf + g = g_2 \tag{2}$$

with $r_g = 0$ or $\deg r_g < \deg f$. Viewing equation (2) from right to left, we see that we may view it also a "result" of the division algorithm (when dividing g_2 by f). Therefore, by the uniqueness of quotient and remainder, we must have

$$q_2 = q + q_g \qquad \text{and} \qquad r_2 = r_g$$

In particular, the remainder terms are the same. This proves existence of the desired g_0, namely, set $g_0 = r_g$.

To prove uniqueness, let $g_0, h_0 \in F[t]$ satisfy the given conditions. By the condition on their residues, $\overline{g}_0 = \overline{g} = \overline{h}_0$, so by definition $h_0 - g_0 \in (f)$, which is equivalent to the existence of $q \in F[t]$ such that

$$h_0 - g_0 = qf \tag{3}$$

By the condition on their degree, and using the fact that F is a field and therefore an integral domain (for the first equality), it follows that

$$\deg q + \deg f = \deg(qf) = \deg(h_0 - g_0) \leqslant \max(\deg h_0, \deg g_0) < \deg f$$

By hypothesis, $\deg f \geqslant 0$, so

$$\deg q < 0$$

which is equivalent to $q = 0$ (in $F[t]$). Substituting this into equation (3), we conclude that $h_0 = g_0$, as desired.

Exercise (b)

Let $f \in F[t]$. Then $F[t]/(f)$ is a field if and only if (f) is maximal.[3] Because $F[t]$ is a principal ideal domain, (f) is maximal if and only if (f) is a nonzero prime ideal,[4] if and only if f is a nonzero prime element,[5] if and only if f is irreducible.[6]

[2] Note that the second condition here is $N(r_g) < N(f)$, rewritten using the fact that the norm function N we have chosen and the degree function deg agree on all nonzero input.

[3] See DF3e, Proposition 7.12, p 254.

[4] See DF3e, Proposition 8.7, p 280.

[5] By definition of a prime element; see DF3e, p 284..

[6] See DF3e, Proposition 8.11, p 284.

Exercise (c)

Let $A = \{1, \ldots, n\}$. Then we may write the given factorization of f into irreducible elements as $f = \prod_{i \in A} p_i$.

By the lattice isomorphism theorem,[7] there exists an inclusion-preserving bijection between the ideals of $F[t]/(f)$ and the ideals of $F[t]$ that contain (f). $F[t]$ is a euclidean domain, and hence a principal ideal domain. Thus, by definition, every ideal of $F[t]$ has the form (g) for some $g \in F[t]$. Also recall that containment relations among principal ideals encode divisibility properties. Specifically, $(b) \subseteq (a)$ if and only if $a \mid b$.[8] It follows that an ideal I of $F[t]$ contains (f) if and only if there exists a subset $B \subseteq A$ and a polynomial $g = \prod_{i \in B} p_i$ such that $I = (g)$, so by the lattice isomorphism theorem, every ideal in $F[t]/(f)$ is the image of such an ideal $(g) \in F[t]$ under the quotient map $F[t] \mapsto F[t]/(f)$.

Exercise (d)

Let $f \in F[t]$. Because $F[t]$ is a principal ideal domain, f is a prime element[9] if and only if f is irreducible.[10] All polynomials of degree 1 are irreducible, [11] and because F is a field, $F[t]$ has at least two polynomials of degree 1, namely, t and $t - 1$. Thus $F[t]$ has at least two prime elements.

Suppose for the sake of contradiction that $F[t]$ has finitely many prime elements, denote them $f_1, \ldots, f_n$. Consider the polynomial

$$f = 1 + \prod_{i=1}^{n} f_i \tag{4}$$

By our argument above, $\deg f \geqslant 2$. Because $F[t]$ is a euclidean domain, it is a unique factorization domain. Therefore f has a factorization into finitely many irreducible elements, say

$$f = \prod_{i=1}^{m} g_i \tag{5}$$

Because $\deg f \geqslant 2$, $m \geqslant 1$. We claim that g_1 (more generally, any g_i) is not associate to any f_i.[12] Suppose for the sake of contradiction that it is. Reindex the f_i so that g_1 is associate to f_1. Then by definition, there exists a $u \in (F[t])^\times \cong F^\times$ such that

$$f_1 = u g_1 \tag{6}$$

Equating the two expressions (4) and (5) for f above, solving for 1, factoring out f_1, and using equation (6), we get

$$1 = \left(u \prod_{i=2}^{m} g_i - \prod_{i=2}^{n} f_i \right) f_1$$

[7] See DF3e, Theorem 7.8, p 246.
[8] See DF3e, p 252.
[9] By definition, prime elements are nonzero. See DF3e, p 284.
[10] See DF3e, Proposition 8.11, p 284.
[11] One can give a quick proof using an argument on the degree of any factorization.
[12] It is sufficient to show that $g_1 \neq f_i$ for any i. (Why?)

This equation shows that $f_1 \in (F[t])^\times$, contradicting the hypothesis that f_1 is irreducible (and hence, by definition, not a unit). Thus g_1 is not associate to any f_i, and therefore g_1 is an irreducible, and hence prime, element of $F[t]$ not in the list $f_1, \ldots, f_n$, as desired.

If F is infinite, then the set $\{t - \alpha \mid \alpha \in F\}$ of polynomials of degree 1 is already a set of infinitely many irreducible, and hence prime, elements.

Exercise (e)

We may give the polynomial ring $F[t]$ the structure of an (infinite-dimensional) F-vector space,[13] with one basis $(1, t, t^2, \ldots)$. In this view, the ideal (f) is an F-subspace; Exercise (a) implies that the quotient space $F[t]/(f)$ has as one basis $(\overline{1}, \bar{t}, \ldots, \bar{t}^{n-1})$, where $\bar{t}$ denotes the image of t under the quotient map $F[t] \to F[t]/(f)$, etc.[14] In particular, $\dim_F(F[t]/(f)) = n$. From linear algebra, we know that a finite-dimensional F-vector space of dimension n is isomorphic to F^n. Therefore, if F is a finite field with q elements, then

$$\#(F[t]/(f)) = \#(F^n) = q^n$$

as desired.

[13] How do we define this structure?

[14] Can you justify these assertions?